



Support de formation

Introduction au Réseau Local



Nom du stagiaire :

Avertissement

Ce support n'est ni un manuel d'utilisation
(pour cela, consultez la documentation jointe à votre logiciel ou micro),
ni un outil d'auto-formation.

Le contenu de ce support a été réalisé à partir de diverses sources mais la principale étant le « Guide des réseau Locaux » de Gérard Mourier.

Ce support est un complément à vos notes personnelles
pour les formations sur la gestion et maintenance micro-informatique.



Sommaire

❑ Introduction

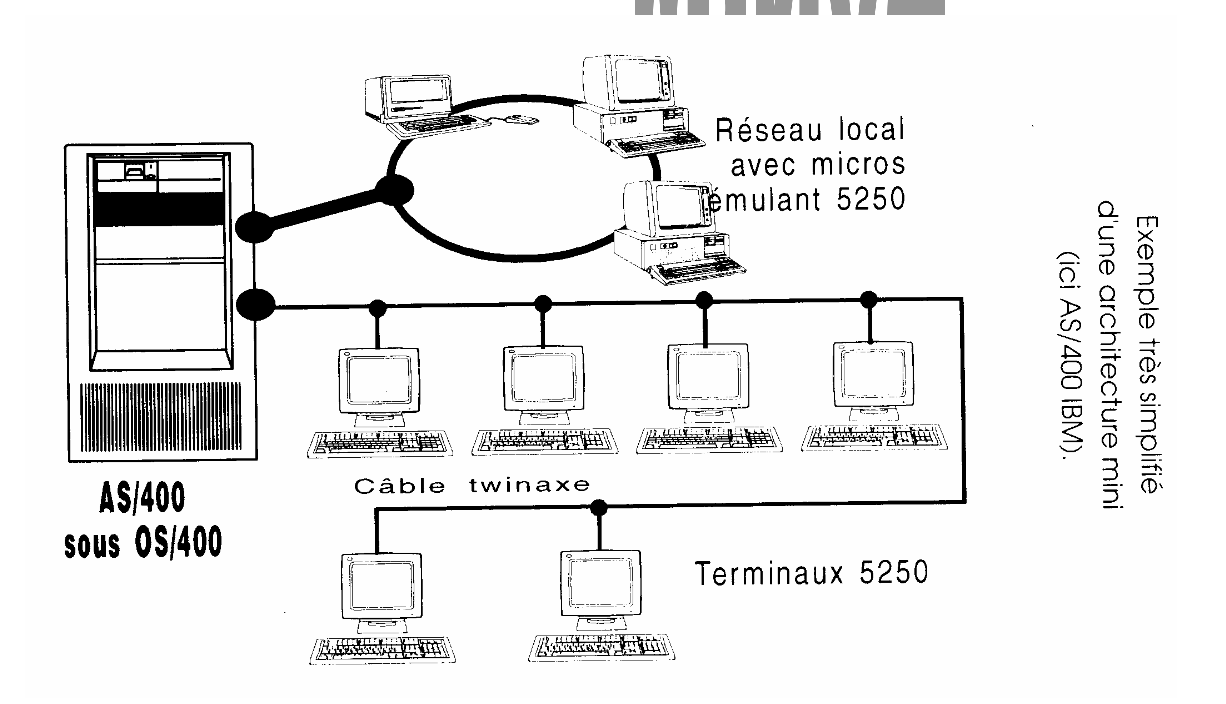
Source « Guide des réseaux locaux – Gérard Mourier » – édition Marabout

Les réseaux locaux possèdent des avantages considérables et de nombreuses activités professionnelles ne pourraient plus être envisagées s'ils n'existaient pas. Cependant, si leur implantation se fait sans trop perturber les utilisateurs (le réseau local est censé leur être « transparent »), il n'en est pas de même pour les ingénieurs et techniciens, chargés de leur installation, de leur mise au point et de leur maintenance.

1. Deux types d'architecture

1.a Grands systèmes et minis

Architecture propriétaire de type centralisé et peu communicante avec les systèmes d'autres constructeurs.
Les utilisateurs s'en partagent la mémoire, les applications, les fichiers, les périphériques et surtout le processeur (temps partagé), entraînant un ralentissement général proportionnel avec le nombre d'utilisateurs. Les accès se font à travers de terminaux passifs.



1.b Stations de travail et micro-ordinateurs

Architecture de type distribué/réparti : les machines sont autonomes et intelligentes à la base et peuvent éventuellement communiquer avec d'autres machines.

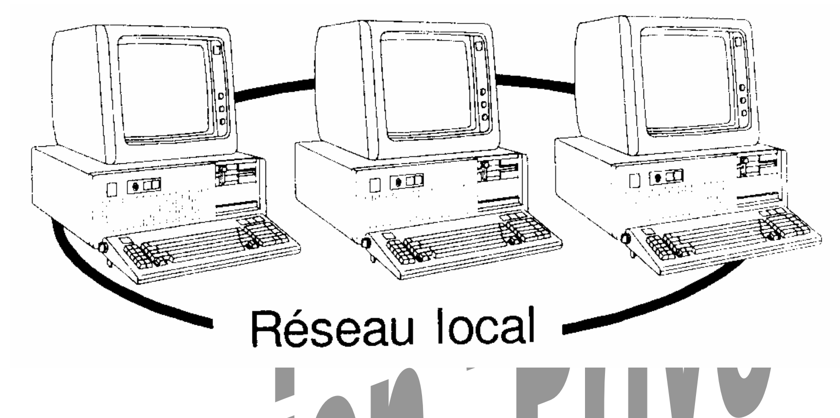
On observe un déclin de plus en plus accentué des minis au profit de ces systèmes non propriétaires et donc au mode « client-serveur ».

2. *Qu'est-ce qu'un réseau local ?*

Un réseau informatique est constitué du maillage de systèmes informatiques interconnectés et sachant communiquer entre eux de manière transparente, même s'ils sont hétérogènes. Il peut parfaitement s'étendre au-delà de l'entreprise (société, école, …).

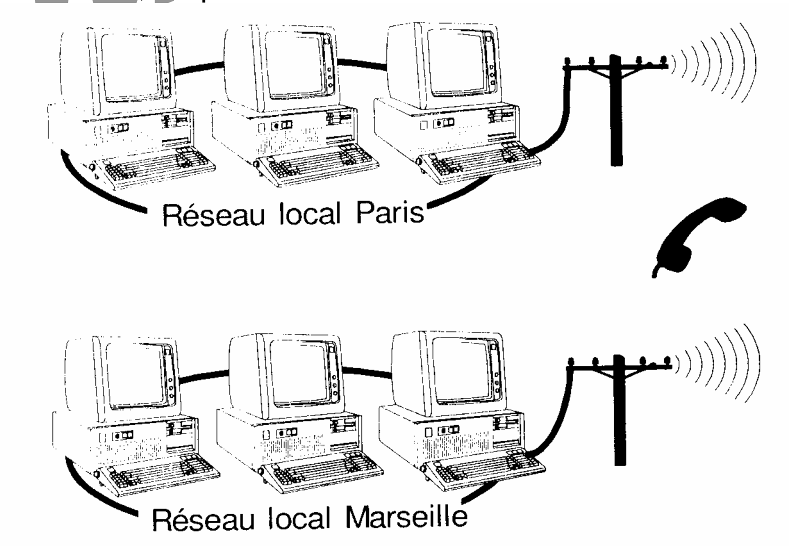
2.a LAN (Local Area Network)

Lorsque les liaisons sont obtenues par câbles ou fibres optiques, on parle alors de « réseau local » ou « LAN ».



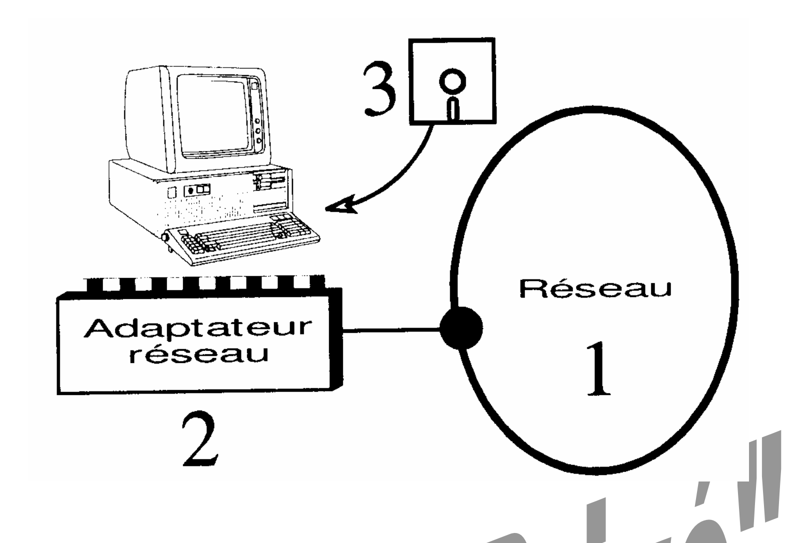
2.b WAN (Wide Area Network)

Lorsqu'elles sont complétées par l'utilisation de liaisons ou lignes, physiques et/ou hertziennes, publiques ou privées, louées aux opérateurs de télécommunication et lorsqu'elles sont distantes, on parle alors de « réseau étendu » ou « WAN ».



Une connexion en réseau local comprend trois éléments principaux :

1. un système de câblage (ex : câble paire torsadée, prise, hub, switch,…)
2. un adaptateur réseau (ex : carte réseau)
3. une couche logiciel adaptée, le système d'exploitation de réseau…



3. *Principaux avantages d'un réseau local*

- Partage de la plupart des ressources informatiques physiques disponibles au sein de l'entreprise, avec des limitations d'usage et une sécurité d'accès plus ou moins importantes : disques ou dossiers partagés, lecteur CD-Rom, imprimantes, modem, fax, …
- Partage d'applications
- Circulation des données plus rapide et plus sûre. Ex : on évite l'utilisation des disquettes.
- Mise en œuvre d'un service de messagerie d'entreprise.
- ….

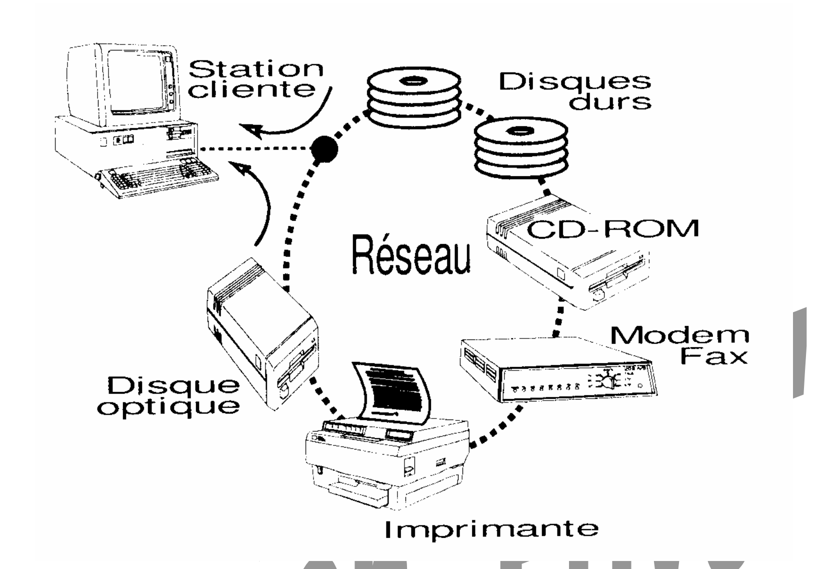
4. Principales contraintes d'un réseau local

- Coût supplémentaire plus ou moins élevé à prévoir selon le système choisi (matériel, logiciel et ses mise à jour périodiques, formation, maintenance).
- Installation et configuration plus ou moins longues, parfois complexes avec certains systèmes, et qui suspendront temporairement l'activité de tous.
- Réorganisation totale de la structure arborescente des répertoires et, presque toujours, réinstallation des logiciels (versions réseaux nécessaires).
- Les machines qui partagent leurs ressources doivent impérativement être sous tension avant les autres et toujours en service, ainsi que ces mêmes ressources.
- Impressions qui peuvent être plus lentes qu'en direct, ainsi que les accès aux différentes ressources, dès lors que le nombre d'utilisateurs est élevé (montée en charge du réseau).
- Politique rigoureuse concernant les risques de virus : logiciel antivirus évolué et régulièrement mis à jours, suppression des lecteurs de disquettes aux postes critiques, etc…
- Consommation de la mémoire sur chaque machine par les fonctions « réseau ».
- Certains réseaux performants nécessitent un « administrateur » à temps complet, disponible sur place ou chez un prestataire de services prêt à intervenir rapidement.
- Enfin, il n'est plus possible de travailler n'importe comment, dans son coin : il faut élaborer une organisation globale du système (disques durs, imprimantes, …) et la respecter scrupuleusement. Cela demandant un minimum de discussion et de formation.

❑ Serveurs et stations

Source « Guide des réseaux locaux – Gérard Mourier » – édition Marabout

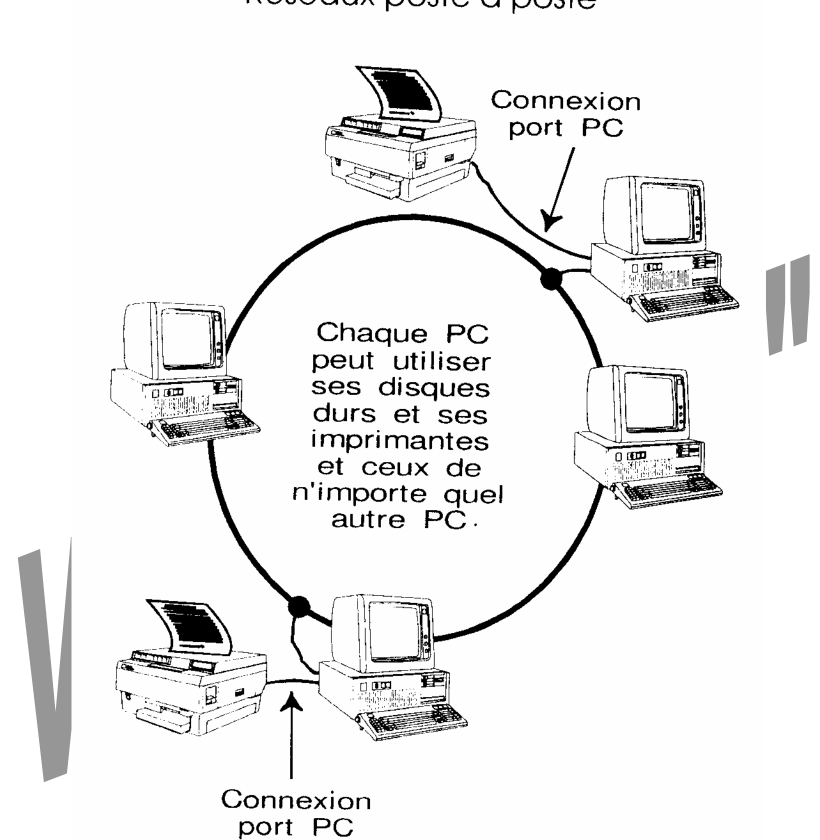
Dans tous les réseaux, les machines qui peuvent mettre leurs ressources physiques et logicielles à la disposition des autres sont appelées « serveurs ».
Cette fonction exige un certain nombre de qualités spécifiques pour un fonctionnement optimal.



Les autres machines reliées au réseau peuvent utiliser sans limitation (*hors cas de stations NT gérant des permissions locales*) leurs ressources propres dites « locales » comme n'importe quel poste de travail individuel (monoposte) et les ressources des serveurs dites « distantes » ou « réseau » qui leur auront été autorisées.
Elles sont alors les « stations clientes » des serveurs.
En théorie, on peut presque considérer que les périphériques des serveurs sont directement et physiquement reliés à chacune des « stations » de manière transparente pour les utilisateurs.

1. Réseaux poste à poste (peer to peer)

Dans un réseau à serveurs non dédiés, « poste à poste » ou encore « égal à égal », toute machine est potentiellement aussi bien un serveur pour les autres machines qu'une « station cliente ».
Ce type de réseau est parfaitement adapté aux petits groupes de travail et aux professions libérales en raison de son bas prix et de sa simplicité d'utilisation.



1.a Principaux avantages des réseaux poste à poste

- Les machines continuent de fonctionner comme avant, sans grande modification, sous leur système d'exploitation originel. On n'a pas besoin de prévoir des machines « gonflées » ou des configurations spéciales.
- La plupart du temps (selon le réseau choisi) un technicien spécialiste est inutile.
- Le coût de base est faible et les évolutions sont faciles et économiques.

1.b Principaux inconvénients des réseaux poste à poste

- Les outils de gestion et de diagnostic livrés avec le système sont généralement peu nombreux et peu puissants et il est rare que des produits complémentaires soient proposés par d'autres sociétés.

- Il n'y a que des outils individuels de détection antivirus : rien ne contrôlant le trafic réseau proprement dit.

- Certains systèmes de sauvegarde très performants sont exclus, ne disposant pas de drivers pour de tels réseaux.

- La sécurité ou les limitations d'accès par les utilisateurs sont plus ou moins élevées selon le logiciel et, dans tous les cas, nettement plus limitées qu'avec un réseau à serveur dédié.

- Lorsqu'on sollicite les ressources d'une machine, on peut ralentir de manière importante le travail de son utilisateur, surtout si on travaille avec de gros fichiers. On évitera donc que trop de fichiers ou de ressources à solliciter soient situés sur une même machine en les répartissant intelligemment ; attention, dans ce cas, il faut prévoir que de nombreuses machines devront alors toujours être sous tension. A cause des mêmes problèmes de ralentissement, le partage d'applications ou l'exécution d'applications à distance (situées sur une autre machine que la sienne) ne sont pas tellement conseillés.

- En plus de la couche logicielle dite « redirecteur client » que possède toute machine utilisant, par le réseau, les ressources d'une ou plusieurs autres (qui sont alors « serveurs dédiés » ou « poste à poste »), les machines « poste à poste » qui partagent leurs ressources (elles sont donc à la fois « stations clientes » et « serveurs ») possèdent une couche logicielle supplémentaire dite « redirecteur serveur » qui consomme une mémoire non négligeable, cela pouvant être un handicap pour les machines fonctionnant sous MSDOS.

- Impossibilité de gérer un sous-système disque à tolérance de panne (RAID – Redundant Array of Inexpensive Disk).

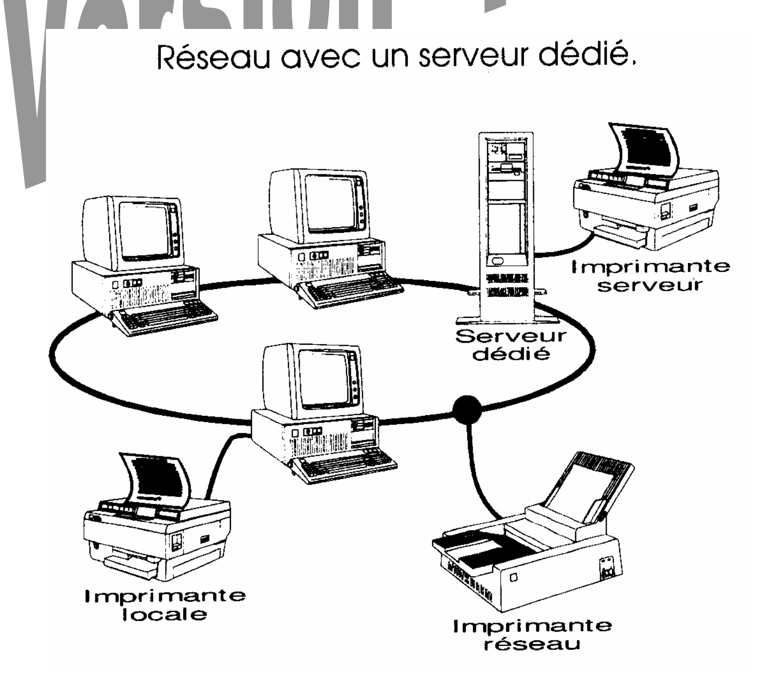
- Les imprimantes ne peuvent (généralement) pas être connectées directement sur le câblage réseau ; elles doivent absolument être reliées à la sortie d'un PC.

- L'administration est rarement centralisée et on risque fort d'avoir un ensemble de machines organisées selon les goûts de chacun (donc ingérables) si des règles précises (telle unité représente la machine d'untel sur toutes les machines, tel répertoire sert à tel usage, etc.) ne sont pas adoptées et respectées.

- La connexion avec d'autres réseaux de machines de la même famille ou entre machines hétérogènes n'est pas toujours possible.

2. Réseaux à serveurs dédiés

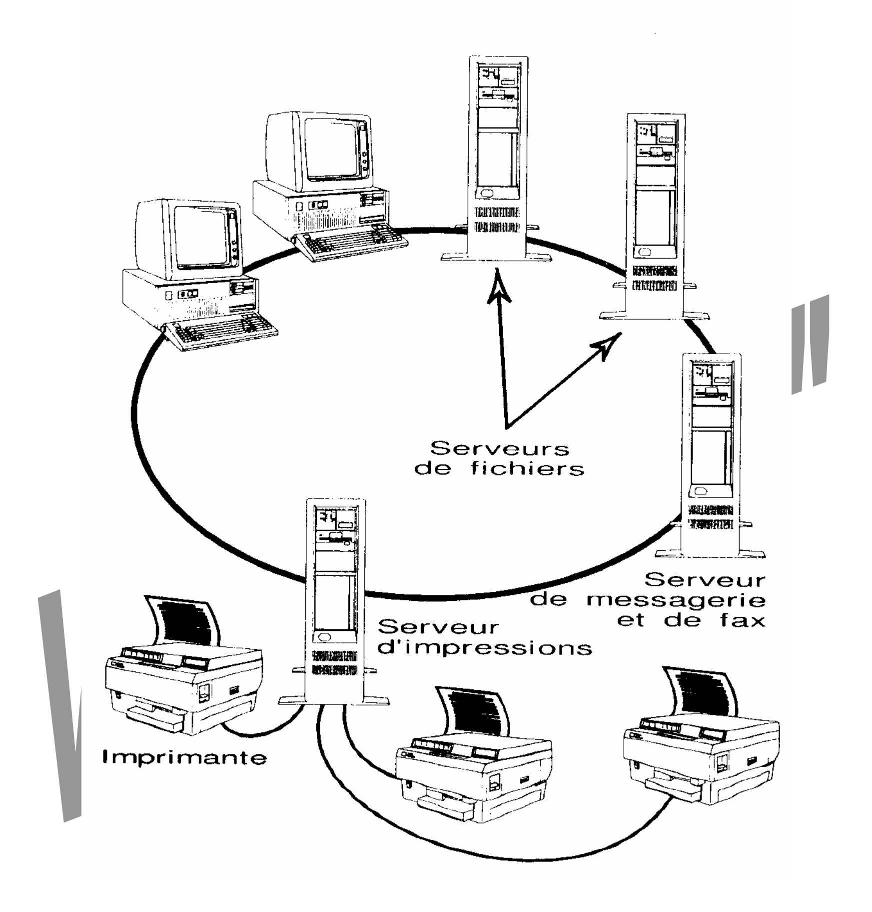
Dans un réseau à serveurs dédiés, on distingue les « serveurs » et les « stations clientes »
Hormis leur connectivité réseau, ces dernières restent des machines classiques, comme celles que l'on aurait utilisées en absence de réseau ou dans un réseau à serveur non dédié dit « poste à poste ».
Aucun utilisateur classique n'est physiquement installé sur les serveurs sinon ces derniers ne seraient plus « dédiés » ! Les serveurs ont alors seule fonction de servir les autres machines.
Ces serveurs ne sont pas des machines ordinaires que l'on aurait simplement « gonflés », ils doivent être optimisés pour ce type de travail : on soigne particulièrement les « entrée-sortie » (E/S ; In/Out, I/O en anglais) ce qui nécessite des bus et des périphériques rapides et un OS multitâche comme Windows NT, Linux, Unix, Netware,…
Ce type de réseau, qui rapproche la « micro-informatique » de la « mini » ou des « grands systèmes » en « centralisant l'information », est très performant et parfaitement adapté aux activités critiques, exigeantes en sécurités de toute nature et à celles qui sont génératrices de transferts de données intensifs (trafic important, car nombreux utilisateurs) ou importants (gros fichiers) à travers le réseau.
En raison de sa complexité et de son coût global (sans oublier les coûts cachés) nettement plus élevés à tous points de vue, il est le plus souvent inadapté (sauf activités lourdes) aux toutes petites structures de deux ou trois machines ; c'est le type même de réseau que l'on utilisera pour gérer l'ensemble du système d'information global de l'entreprise. Dans certains cas, il est possible d'y rattacher des groupes de travail en réseaux poste à poste.



De nombreux réseaux, petits ou moyens, ont un unique « serveur dédié » il fait alors simultanément fonction, comme pour les réseaux « poste à poste », de serveur de fichiers, de serveur d'impression et de serveur de messagerie et/ou de Fax.

Dès que le nombre de machines connectées est élevé et que l'on prévoit un trafic réseau important, il est préférable de spécialiser des serveurs, tant pour éviter les goulots d'étranglement que les blocages intempestifs du système (une impression ou une émission de télécopie qui pose problème pourra totalement bloquer certains serveurs). Ces serveurs spécialisés sont la plupart du temps des micro-ordinateurs ou des stations de travail sur lesquels tournent en exclusivité des utilitaires spécifiques, livrés avec le système d'exploitation du serveur ou encore produits par une société tierce.





On dit souvent que ces réseaux travaillent en mode « client-serveur » ; en vérité, si les applications sont bien situées sur le serveur, elles sont le plus souvent exécutées (à distance) par les stations clientes, qui doivent en avoir techniquement la capacité (même environnement logiciel, mémoire, affichage, rapidité) : on travaille alors en mode « serveur de fichiers ».

On peut véritablement parler de « client-serveur » lorsque les applications, le plus souvent des bases de données haut de gamme comme Sybase, Oracle, SQL server, Access sont exécutées par le serveur lui-même, donc développées spécialement pour son système d'exploitation propre et présentes dans sa mémoire (qui doit être étendue en conséquence). On comprend bien la différence de rapidité qui peut en résulter pour les « requête » effectuées par les utilisateurs.

Dans la pratique, on combine le mode « client-serveur » pur et dur et le mode « serveur de fichiers » : l'application est bien exécutée sur le serveur, mais de nombreuses opérations annexes ou techniques sont réalisées par les stations clientes elles-mêmes afin de limiter

la charge processeur du serveur, limitant ainsi l'attente des utilisateurs (comme ce pouvait être le cas sur les systèmes totalement centralisés, « minis » et « grands systèmes »).

2.a Principaux avantages des réseaux à « serveurs dédiés »

- Les disques durs utilisés (par les serveurs) sont le plus souvent en technologie SCSI cela permet un chaînage de façon à n'avoir virtuellement qu'une seule unité et le support des sous-systèmes à tolérance de panne (RAID) courants.

- Les outils de gestion et de diagnostic disponibles sur le marché sont très nombreux et très évolués.

- De nombreuses « passerelles » sont disponibles pour communiquer avec les autres réseaux, en local ou de façon distante, et des « clients » (logiciels pour qu'une machine devienne une station cliente) sont disponibles pour la plupart des systèmes d'exploitation.

- Des « antivirus dédiés réseau » et des « systèmes de sauvegarde centralisés » très évolués sont proposés par de nombreuses sociétés.

- Les performances globales sont très supérieures à celle des réseaux « poste à poste ». Le goulot d'étranglement est nettement moins marqué qu'avec les serveurs des réseaux « poste à poste » (ralentissement lors de la montée en charge, c'est-à-dire des augmentations de connexion et de trafic).

- Sécurités d'accès et de fonctionnement centralisées, pouvant être absolues.

- Possibilité de spécialiser les serveurs, afin d'améliorer les performances et la fiabilité.

- Possibilité de mettre en oeuvre des imprimantes spéciales réseau. Elles recevront et traiteront les données beaucoup plus rapidement qu'à partir d'un port parallèle ou série et pourront être installées n'importe où (au plus près des utilisateurs), grâce à leur connexion directe sur le câble réseau.

- On n'a pas besoin de se préoccuper de maintenir sous tension toutes les machines qui contiennent les données utiles ou qui alimentent telle ou telle imprimante, comme avec les réseaux « poste à poste ». Puisque les données sont toujours situées uniquement sur le disque dur de chaque station cliente ou sur les serveurs, il suffit que ces derniers soient alimentés (dans la plupart des cas, ils sont sous tension 24h/24h).

2.b Principaux inconvénients des réseaux à « serveurs dédiés »

Quoique considérablement plus performant à tous points de vue, un réseau à « serveurs dédiés » (ou « spécialisés ») est beaucoup plus cher à l'achat, demande impérativement une alimentation de secours par onduleur et profitera d'un système à tolérance de panne (RAID 1 au minimum). Il est aussi beaucoup plus complexe qu'un réseau « poste à poste » et, de ce fait, surprend souvent par ses nombreux et importants coûts visibles ou cachés on citera notamment :

- Sous-traitance des opérations d'installation, de configuration, de modification / ajout, d'administration et de maintenance (ces deux dernières réclament une présence potentielle permanente) Si on veut réaliser ces tâches en interne, il faudra procéder à des embauches de personnels spécialisés réseau ou prévoir des formations nombreuses, longues, coûteuses et régulièrement répétées dès « techniciens maison », à quoi il faudra ajouter des abonnements aux supports techniques constructeur (car les difficultés peuvent être nombreuses).

- Mises à jour des logiciels du réseau et de leurs extensions, des antivirus et des sauvegardes.., payées le plus souvent en fonction du nombre d'utilisateurs potentiels.

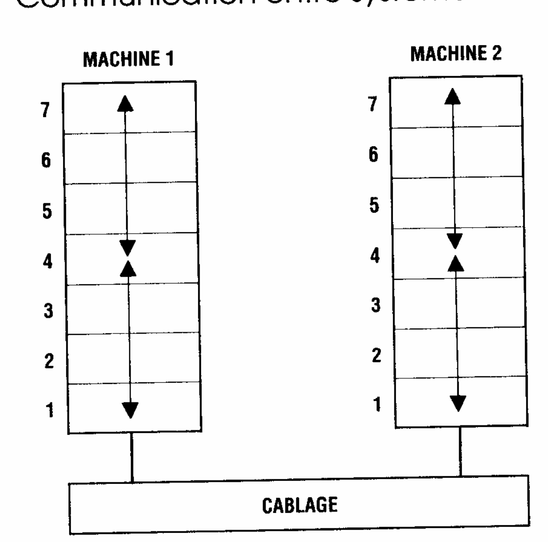
❑ Le Modèle OSI (Open System Interconnection)

Devant la nécessité de parvenir à une interopérabilité des solutions réseau incompatibles, l'ISO (International Standards Organisation), représentée en France par l'AFNOR (Association Française de NORmalisation) et aux USA par l'ANSI (American National Standards Institute), a proposé en 1984 son modèle officiel dit OSI.
Ce modèle est constitué de 7 couches.

7	Application	Couches « hautes » applications réseau	Traitement de l'information
6	Présentation		
5	Session		
4	Transport	Couches « moyennes » réseau physique de transport	Transport de l'information
3	Réseau		
2	Liaison	Couches « basses » réseau physique de transport	
1	Physique (adaptateur réseau et câblage)		

Modèles de référence OSI en couches

Ce modèle harmonise le processus général de communication en le découpant en sept couches fonctionnelles structurées.
Chaque couche du modèle OSI s'appuie sur l'ensemble des services apportés par les couches inférieures mais n'a de contact (ou dialogue) direct qu'avec la couche immédiatement inférieure (qui lui offre ses services) et immédiatement supérieure (à qui elle offre ses propres services).



Aucun contact direct n'existe donc entre les couches homologues de deux machines qui échangent des informations ; celles-ci transitent toujours à travers l'ensemble des couches, de couche en couche, selon des règles très précises appelées « protocoles ».

Ce cloisonnement et cette spécialisation des fonctions évitent d'aboutir à un modèle qui serait figé ; les couches de même position étant (théoriquement) interchangeables, on peut donc facilement s'adapter à un nouveau standard matériel ou logiciel en développant une nouvelle couche de remplacement, sans avoir pour cela à repenser toutes les autres couches.

Dans la pratique, on ne peut pas dire que tous les systèmes respectent strictement le modèle OSI (surtout à partir de la couche 3) ; dans certains cas, des couches débordent sur d'autres couches, d'autres sont escamotées et remplacées par une couche globale et parfaitement monolithique, donc indissociable en sous-couches au modèle OSI.
D'autre part, toutes les couches développées pour occuper un même niveau n'apportent pas forcément les mêmes services.

1. Rôles des différentes couches du modèle OSI

1.a Couche 7 - Application

C'est l'interface entre l'utilisateur ou les applications et le réseau ; elle concerne donc, entre autres : messagerie, transfert de fichiers, émulation de terminaux, partage de fichiers, etc.

1.b Couche 6 - Présentation

La couche présentation convertit l'information purement électronique (dite interne) pour lui faire adopter sa forme finale, celle que vont comprendre les applications et les utilisateurs (syntaxe, sémantique, cryptage, compression, conversion des caractères graphiques et semi-graphiques, format des fichiers, etc..). Elle assure éventuellement cryptage (sécurisation) et compression (réduction des durées de transfert).

1.c Couche 5 - Session

Cette couche est responsable de la gestion et de la sécurisation du dialogue (noms d'utilisateurs, mots de passe, etc..) entre les divers équipements, applications et utilisateurs en réseau. Elle assure la reprise en cas d'incident. L'unité d'information de cette couche est la « transaction ».

1.d Couche 4 - Transport

Cette couche, peut être comparée à un centre de tri postal. Elle segmente les données qui lui viennent de la couche précédente (n°5), quand elles dépassent la taille des « buffers » mémoire utilisés, puis prépare et contrôle le travail des « postiers » (couche n°3) à qui elle confie ces données segmentées. Elle est capable de multiplier les voies d'accès et corrige les erreurs de transport.

1.e Couche 3 - Réseau

Cette couche traite la partie « données utiles » contenue dans la « trame ». Elle connaît l'adresse de tous les destinataires et choisit l'itinéraire le plus approprié pour assurer leur acheminement, en fonction de l'état du réseau, de certaines priorités, etc. Elle gère donc l'adressage, le routage et le contrôle de flux.

1.f Couche 2 - Liaison

C'est au niveau de cette couche qu'est définie l'unité basique de l'information qu'on appelle « trame » (c'est le véhicule qui va contenir l'information). Comme pour toute transmission sérielle, elle comprend des bits de données (bits utiles venant des couches supérieures) encadrés par des bits techniques (dont l'adresse du noeud destinataire). La composition et l'organisation d'une trame (son format) varient totalement selon le standard (certains disent l'architecture) du réseau (physique) choisi et, donc, de l'adaptateur réseau utilisé on trouve même des trames différentes (variantes) dans un même standard.

La couche liaison est responsable de l'acheminement sans erreur des trames ; elle effectue des contrôles et des corrections des erreurs de transmission, la régulation du flux de données pour éviter de saturer les équipements dont elle est très proche comme la couche n°1.

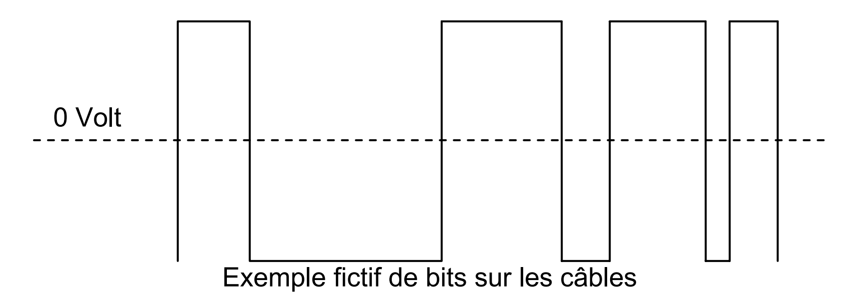


0	0	Emetteur	Destinataire	Données	1	0

Exemple de trame fictive

1.g Couche 1 - Physique

La couche physique génère les signaux électriques - ce ne sont pas directement des niveaux binaires, 0 ou 1, trop sensibles aux perturbations parasites - qui serviront de support aux flux de données proprement dites et issues des couches supérieures (le tout est donc codé). Ces signaux dépendent des caractéristiques propres de l'adaptateur réseau.
La couche physique traite de la même façon, mais en sens inverse, les signaux électriques venant d'autres machines, en les transmettant à la couche n°2 (après décodage). Son niveau d'intelligence est rudimentaire, elle traite les bits logiques qui la parcourent, sans comprendre leur organisation et/ou leur signification.



Exemple fictif de bits sur les câbles

2. En résumé

Le modèle de référence OSI préconise le découpage de la communication en 7 couches.

Chaque couche a un rôle bien particulier et communique sur requête (sur demande) de la couche supérieure en utilisant la couche inférieure (sauf pour la couche physique 1).

Un exemple d'utilisation du modèle OSI est le protocole TCP/IP qui signifie TCP sur IP, TCP étant un protocole de niveau 4 (transport) s'appuyant sur IP qui est un protocole de niveau 3 (réseau).
Ainsi TCP demande l'utilisation d'IP pour échanger des informations, et IP est donc utilisé par TCP.

3. Liens internet sur OSI

http://perso.wanadoo.fr/vincent.zemb/osi/

http://www.guill.net/reseaux/Res1Intro.html



❑ Les Câbles

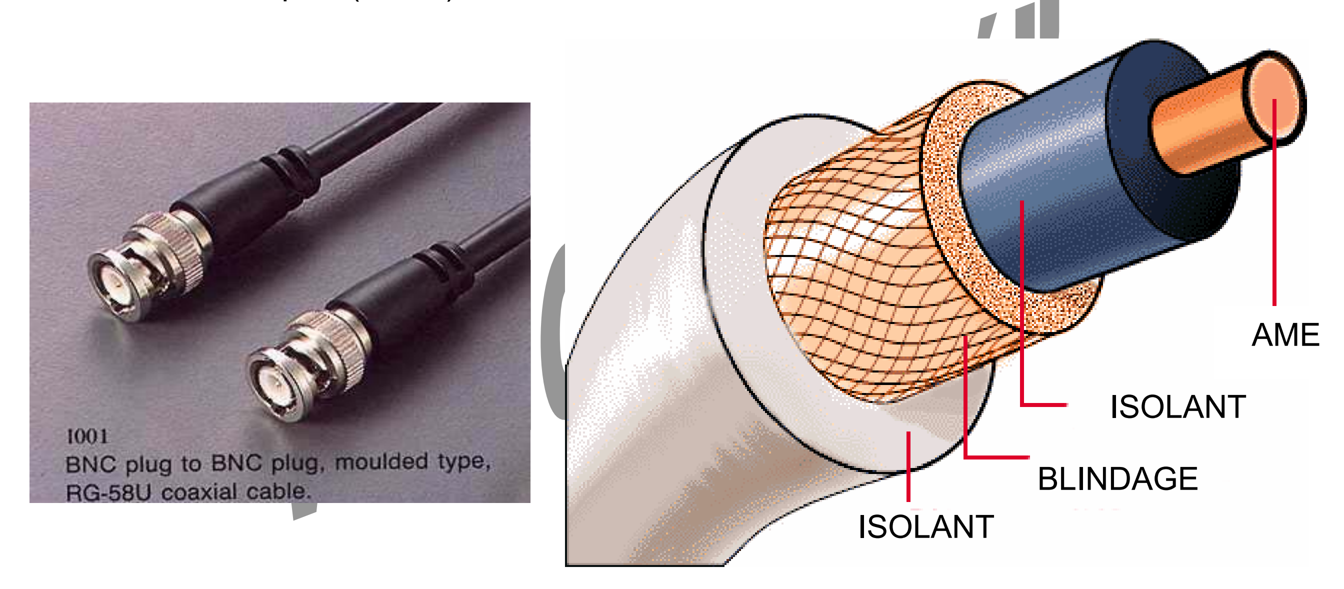
Définition : câble destiné exclusivement au transport de données numériques (donc à des courants faibles).

Les principaux véhicules de l'information entre machines reliées en réseau local appartiennent à trois grandes familles de câbles :

1. Coaxial
2. Paires torsadées
3. Fibres optiques

1. Câbles blindés coaxiaux

Les câbles électriques (cuivre) blindés coaxiaux ressemblent aux câbles TV.



Malgré de bonnes qualités intrinsèques (notamment leur faible sensibilité aux perturbations électromagnétiques ou parasites), ils sont de moins en moins utilisés et laissent de plus en plus la main aux paires torsadées.

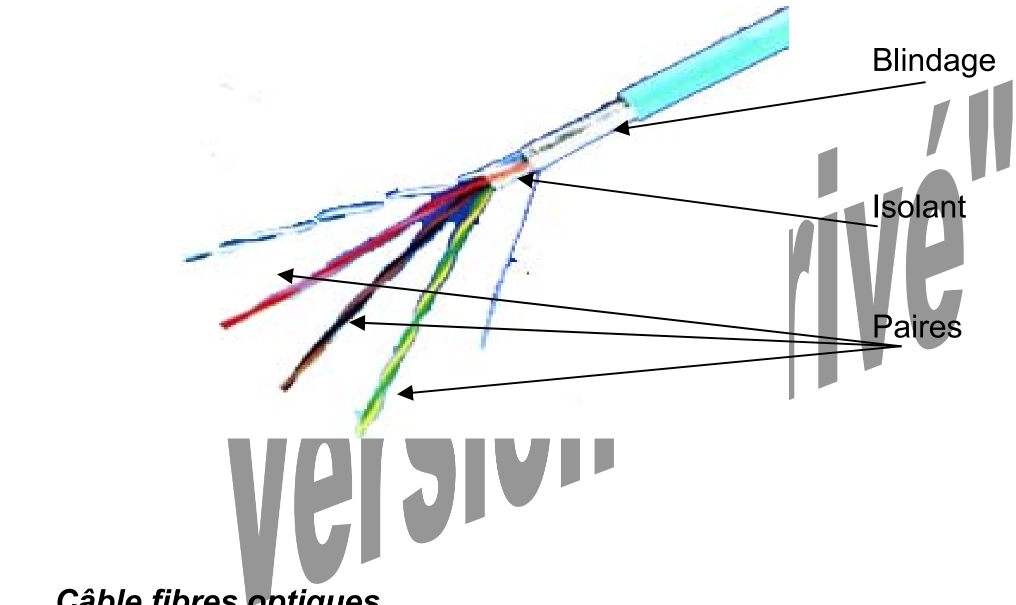


Terminaison

2. Câbles paires torsadées

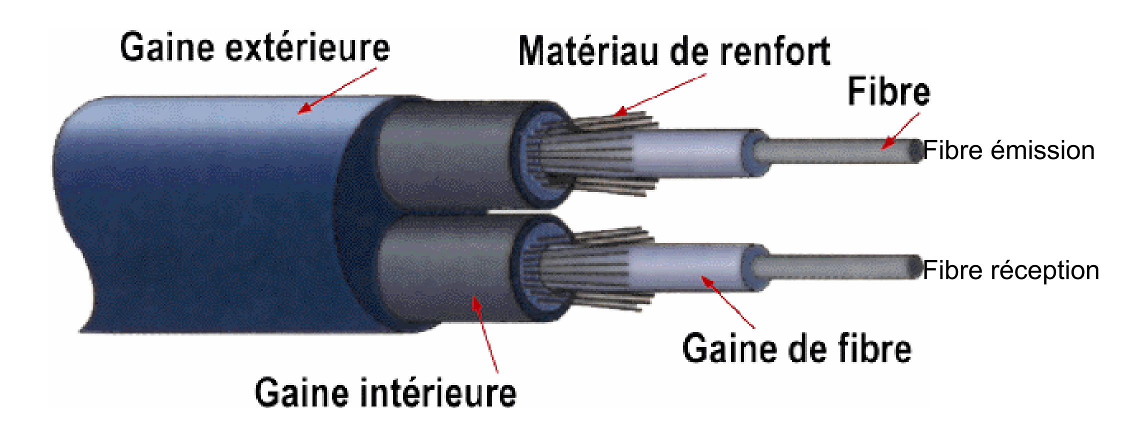
Les câbles électriques (cuivre) à paires torsadées ressemblent très fortement aux câbles téléphoniques.

On notera que les torsades diminuent la sensibilité aux perturbations électromagnétiques, la diaphonie (mélange de signaux entre paires) et l'atténuation du signal tout au long du câble.
Il existe des versions blindées (STP) et non blindées (UTP).
Les câbles à paires torsadées sont actuellement, et de loin, les plus employés, en raison de leur prix raisonnable, mais surtout à cause des architectures physiques mises en oeuvre avec ces câbles, celles-ci s'adaptant nettement mieux aux câblages de groupes de travail et aux pré-câblages d'immeubles de bureaux.



3. Câble fibres optiques

Les câbles à fibres optiques transmettent les informations par modulation d'un faisceau lumineux.



Les câbles à fibres optiques ont de nombreux avantages :

- ils sont extrêmement rapides et peuvent transmettre une grande quantité d'informations à la fois (bande passante élevée).
- ils sont intrinsèquement insensibles à toute interférence électromagnétique et n'en génèrent pas eux-mêmes.
- ils génèrent très peu d'atténuation sur le signal (lumineux), ce qui permet d'utiliser un segment unique de très grande longueur : plus d'un kilomètre avec une émission **multimode** (diode électroluminescente LED émettant dans le visible), plus de 10 km avec une émission **monomode** (LED Laser infrarouge).
- ils sont très peu encombrants et nettement plus légers que les câbles en cuivre.
- ils ne peuvent absolument pas générer la moindre étincelle, ce qui les fait adopter d'office dans les environnements explosifs.
- ils assurent intrinsèquement une meilleure confidentialité des données (difficulté de réaliser une connexion pirate efficace).

Cependant, en raison de leur coût global élevé (adaptateur, câble, installation, réglages délicats, contrôles, etc.), leur utilisation dans les réseaux locaux standard est plutôt réservée aux « épines dorsales » (« backbones »), c'est-à-dire aux arrivées centrales ou générales d'immeubles ou de gros services ou encore lorsqu'une bande passante considérable est indispensable (multimédia, visiophonie, transmission de très gros fichiers, etc.). Il faut impérativement sous-traiter leur mise en oeuvre auprès de spécialistes expérimentés et hyper-équipés en appareillage de mesure, d'autant plus que les longueurs utilisées ne permettent pas de trouver des câbles standard tout montés, comme c est souvent le cas avec les câbles électriques.

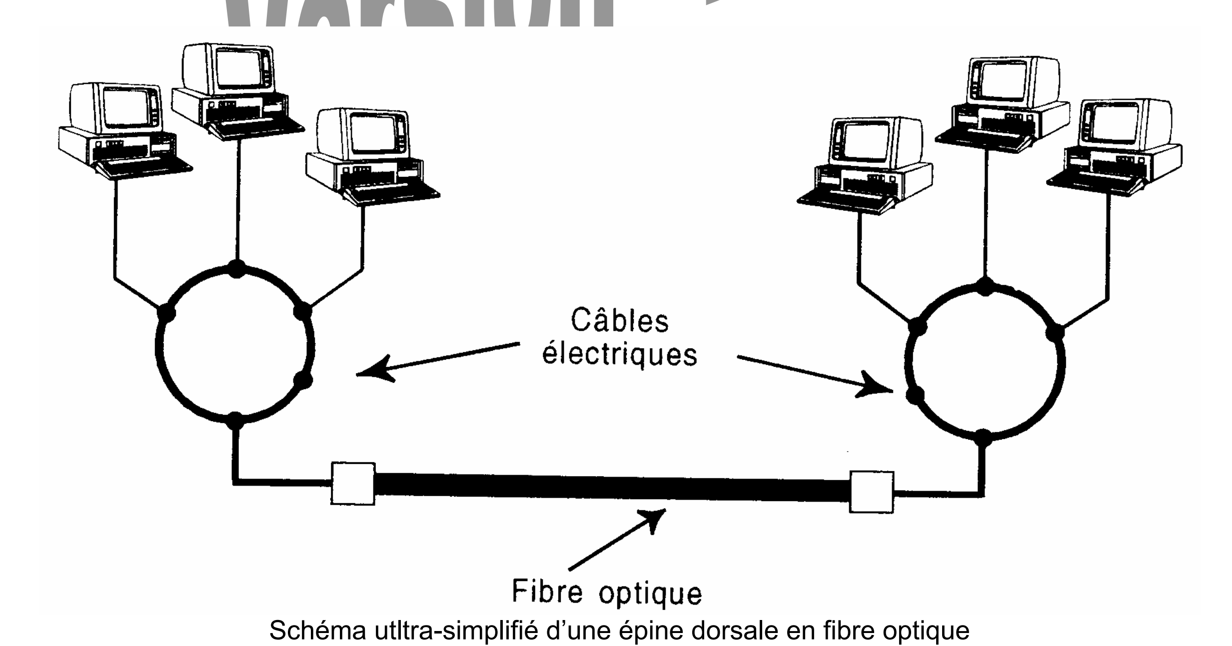


Schéma utltra-simplifié d'une épine dorsale en fibre optique

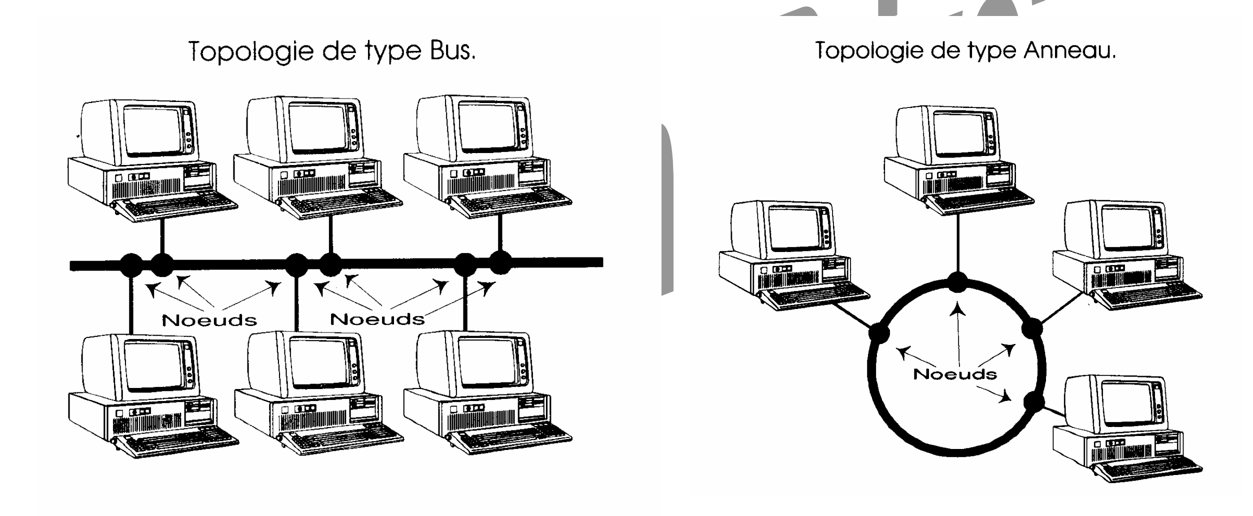
❑ Topologie

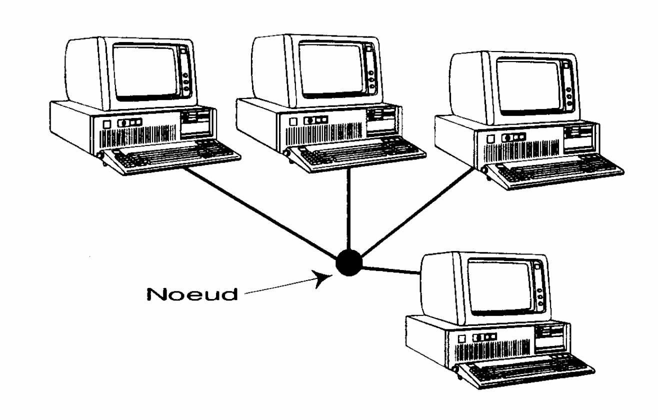
La topologie désigne la façon dont les diverses machines d'un réseau sont interconnectées, ce mot étant à prendre au sens large.

Il faut distinguer la « topologie logique » ou réelle (celle que voit le réseau lorsqu'il regarde les machines) et la « topologie physique » ou apparente (celle que voit l'utilisateur lorsqu'il suit les chemins de câbles).

Souvent la « topologie physique » et la « topologie logique » peuvent se trouver soit confondues, soit différentes, soit combinées.
Par exemple, certains systèmes appartiennent à une même topologie logique (celle qui est importante pour le réseau et pour comprendre comment circule l'information), alors qu'ils mettent en oeuvre une topologie physique (celle qui est importante pour comprendre comment raccorder électriquement les machines) différente.

Les topologies les plus répandues dans les réseaux locaux sont le **bus**, **l'étoile** (star) et **l'anneau** (ring).





1. Méthode d'accès

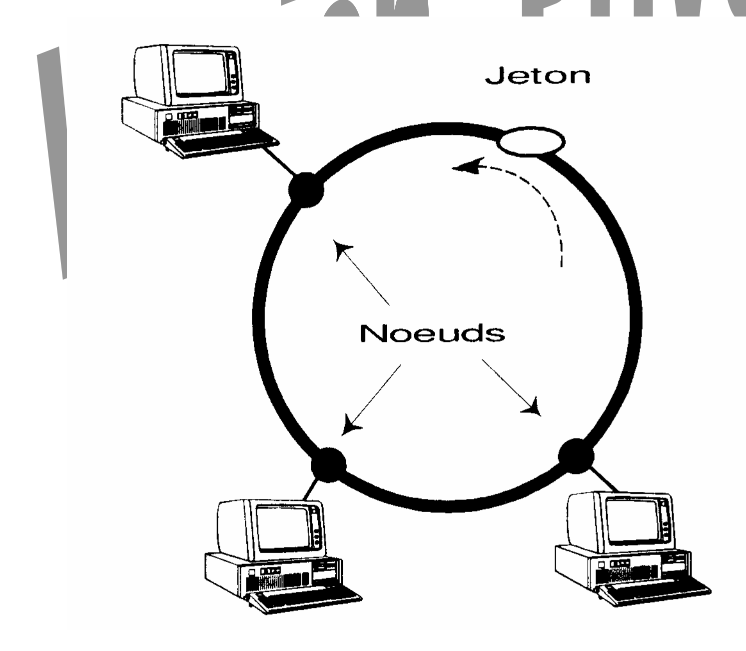
La méthode d'accès désigne les moyens utilisés pour organiser et réglementer la circulation des informations.
Quel que soit le réseau local utilisé, une seule machine à la fois peut normalement être autorisé à émettre sur le câble réseau. Il existe donc plusieurs méthodes qui gèrent de manière différente les conflits d'accès.
Deux grandes familles de méthode :

- « déterministes » : elles s'arrangent pour éviter ces conflits en donnant à l'avance une autorisation d'émettre (coopération entre machine). On peut citer la méthode du **jeton** (802.5).

- « aléatoires » (ou non déterministes) : elles ne peuvent pas garantir le temps que met une information pour aller d'un nœud du réseau à un autre. Elles acceptent les conflits (générateurs de « collisions » sur le câble) mais savent intrinsèquement les gérer. On peut citer la méthode **CSMA/CD** (802.3)

1.a Méthode d'accès du jeton

Cette méthode d'accès est essentiellement utilisée dans les réseaux organisés selon la topologie (logique) en « anneau »

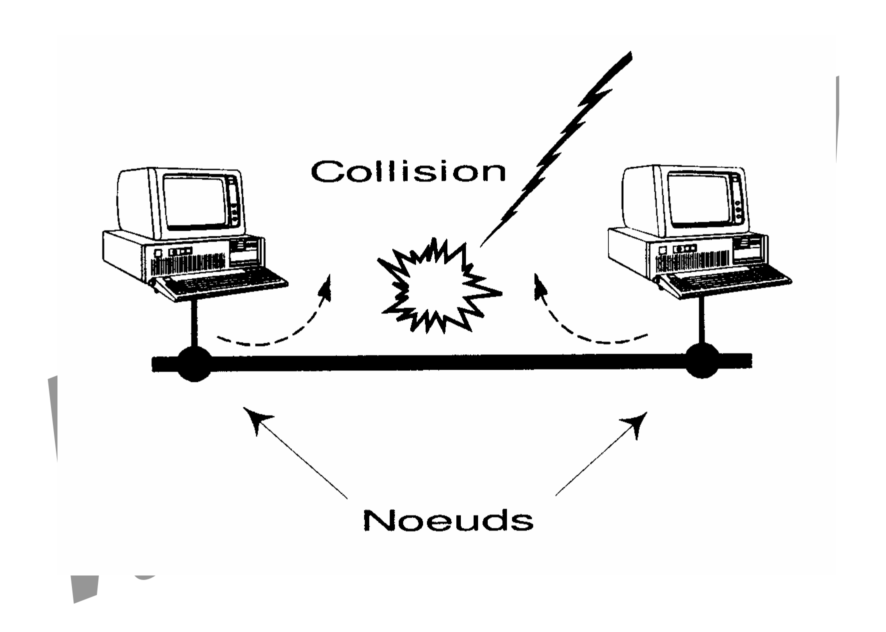


Un jeton (trame logicielle) circule en permanence, toujours dans le même sens, traversant toutes les machines (ou noeuds) de l'anneau. Pour qu'une machine puisse émettre une trame sur l'anneau, elle doit s'emparer du jeton (qui devient occupé) lorsqu'il passe à sa portée, ce qui peut nécessiter l'attente du temps nécessaire pour qu'il parcoure un tour complet. La trame émise traverse chaque machine qui contrôle si elle lui est destinée (en lisant le champ destination de la trame) si ce n'est pas le cas, elle la transmet à la machine suivante après l'avoir régénérée (simple remise en forme électrique du signal) ou la marque mauvaise si elle contient des erreurs.

Enfin, la machine à qui était destinée la trame la transmet aux couches supérieures OSI qui vont décoder son sens et la traiter. La trame continue son parcours et revient à la machine qui l'a émise ; celle-ci va vérifier si elle a été correctement reçue par la machine destinataire, puis la détruit.
Dans les systèmes les plus basiques, c'est seulement à ce moment que le jeton est libéré, afin qu'il puisse être utilisé par une autre machine (il a fallu attendre un tour complet) ; dans les systèmes plus évolués, le jeton est libéré dès que la trame est parvenue à la machine destinataire.

1.b Méthode d'accès CSMA/CD

La méthode d'accès CSMA/CD (CSMA = Carrier Sense Multiple Access ; CD = Collision Detection) est utilisée dans les réseaux organisés selon la topologie (logique) dite en « bus ».



Dans cette méthode, chaque machine qui veut émettre peut le faire librement après avoir simplement vérifié (en écoutant le trafic) qu'aucune trame ne circule.
Cependant, une collision des trames peut parfaitement arriver, soit à cause des délais inégaux de transmission sur le câble ou parce que deux machines ont décidé bien involontairement d'émettre en même temps. Les deux machines émettrices, qui écoutent toujours le réseau, détectent évidemment cette anomalie, remplacent la suite des trames par des bits de renforcement de collision, afin que tout le réseau ait le temps de comprendre ce qui vient de se passer. CSMA/CD leur permet de recommencer leurs émissions après un très court laps de temps déterminé de façon aléatoire, afin d'être sûr qu'il sera différent pour chaque machine (sinon les collisions se reproduiraient à répétition).

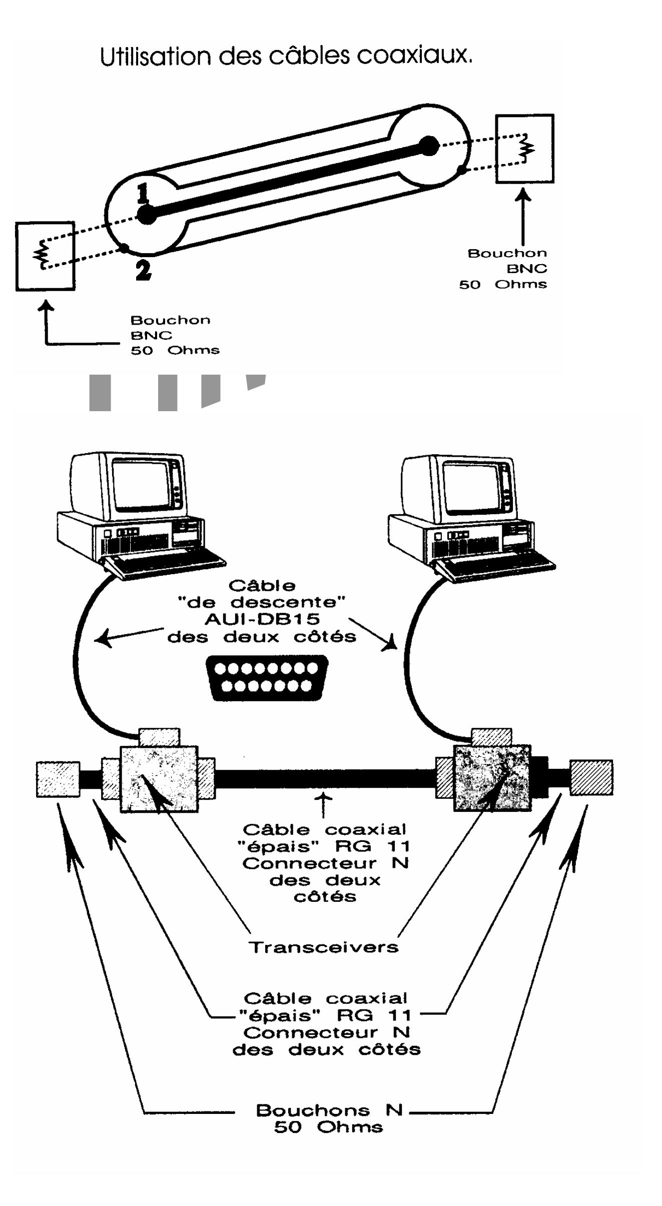
❑ Standards de réseaux physiques

1. Ethernet 10 Mbits/s

Ethernet est basé sur une topologie logique de type « bus ». Les trames émises sont diffusées en parallèle à tous les nœuds du réseau.
La méthode d'accès est CSMA/CD.
La vitesse théorique est de 10 Megabits par seconde mais le débit réel des informations est beaucoup plus faible.

1.a 10 base 5 - Ethernet standard - Thicknet - Gros

C'est le premier « ethernet » qui a été proposé et le moins utilisé aujourd'hui.
Il utilise un câble coaxial d'impédance 50 ohms avec une topologie physique en « bus ». Les extrémités reçoivent un « bouchon » ou « terminaison » de 50 Ω fermant ainsi le circuit pour que le courant circule.



Limites de l'ethernet 10 base 5 :

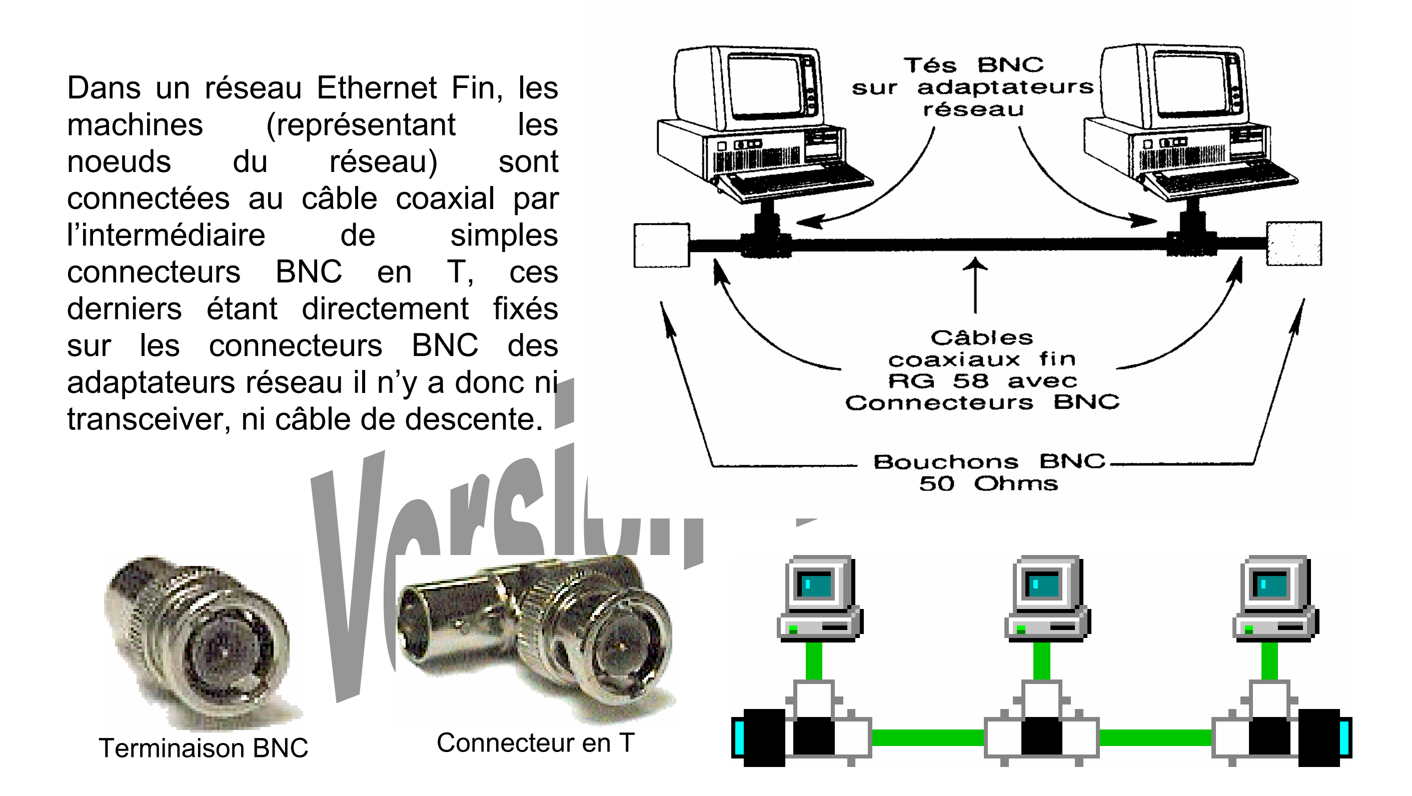
- 500 m max de chaque segment
- 100 transceivers (émetteur-récepteurs connectant les machines au câble coaxial) max sur le câble principal
- 2,5 m au minimun entre 2 transceivers
- 50 m max pour les câbles de descente

1.b 10 base 2 - Ethernet fin - Thinnet - Thin

10 Base 2 est l'Ethernet le plus facile et le plus économique à mettre en oeuvre, c'est pourquoi il est très répandu dans les tout petits réseaux ; cependant, il est menacé de disparition au profit de câblages à paires torsadées comme 10 Base T.

Comme pour 10 Base 5, c'est encore un coaxial d'impédance 50 Ω (mais moins performant), sur une topologie physique en « bus » (bouchons de 50 Ω), mais son diamètre est plus petit (5 mm), sa couleur est noire. On notera que les bouchons, comme tous les connecteurs reliés directement à ce câble, sont de type « BNC ».

Dans un réseau Ethernet Fin, les machines (représentant les noeuds du réseau) sont connectées au câble coaxial par l'intermédiaire de simples connecteurs BNC en T, ces derniers étant directement fixés sur les connecteurs BNC des adaptateurs réseau il n'y a donc ni transceiver, ni câble de descente.



Terminaison BNC

Connecteur en T

Attention ! Pour toute technologie physique en « bus », on risque de bloquer toutes les machines en cas de problème comme la coupure ou l'écrasement du câble ou la déconnexion d'un connecteur BNC.

Limites de l'ethernet 10 base 2 :

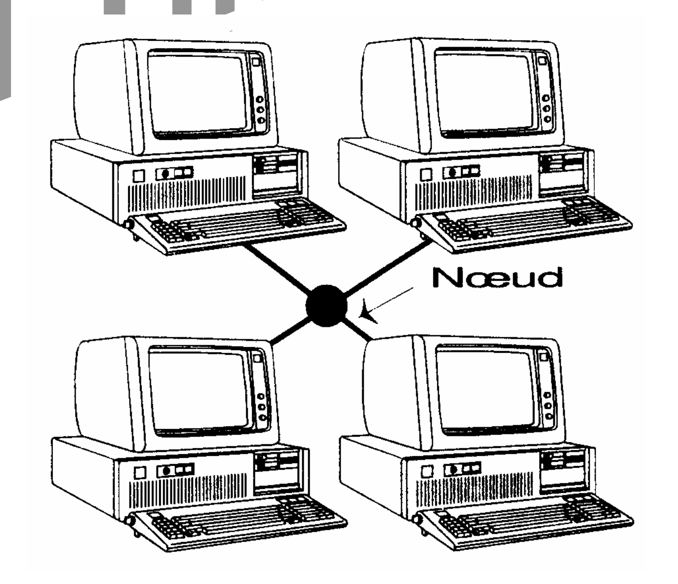
- **185 m** pour chaque segment
- 30 noeux (T) max sur le câble principal

1.c 10 base T

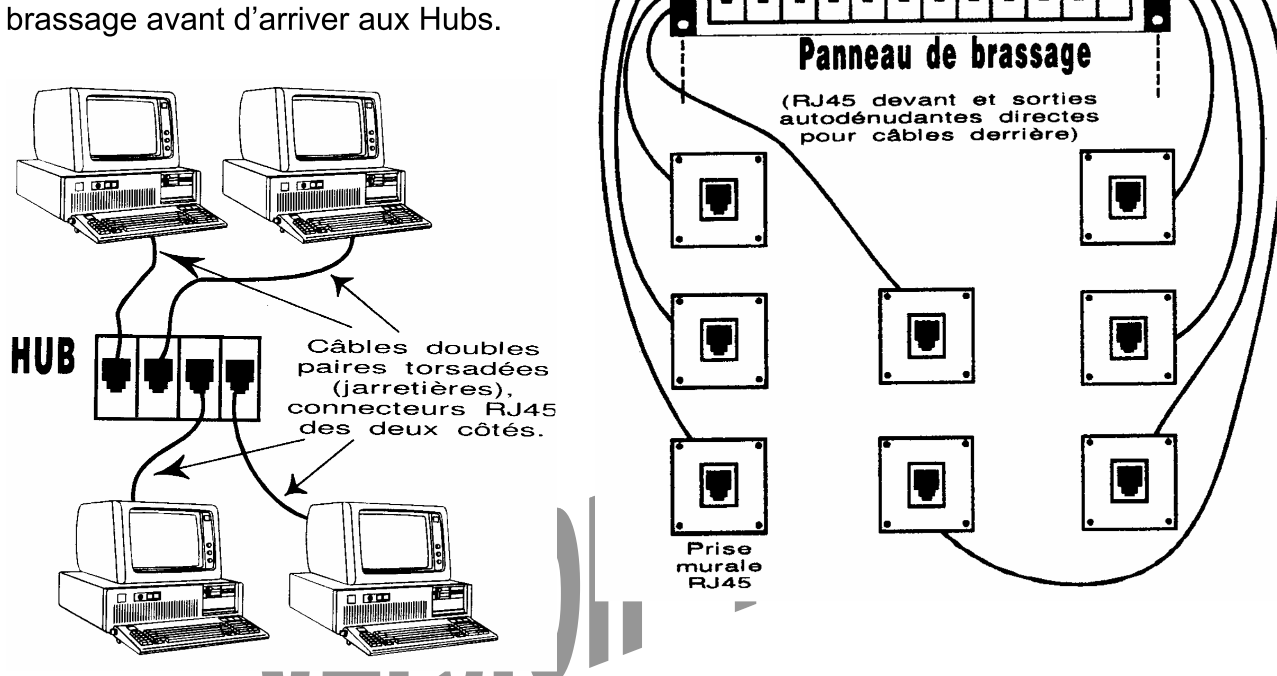
L'Ethernet 10 Base T, n'est ni le plus facile à mettre en oeuvre ni le plus économique à priori ; c'est cependant le plus en vogue car ses avantages sont fondamentaux, notamment dans le cas de grands et moyens réseaux :

- Il convient parfaitement au précâblage des immeubles (installé lors de la construction), puisque son câble suit les mêmes règles d'installation que celui du téléphone.
- Le câble et les connecteurs utilisés, très proches de ceux du téléphone, sont peu coûteux.
- Il facilite l'organisation physique en groupes de travail.
- En cas de coupure ou de débranchement accidentel du câble de raccordement d'une machine, on ne risque pas un blocage de tout le réseau : seule la machine est affectée (c'est pratique pour les machines volantes).
- Il est possible d'inclure une protection automatique (paramétrable par logiciel) supplémentaire en cas d'adaptateur réseau devenu bavard (panne irrémédiable qui provoque des collisions ininterrompues), isolant la machine responsable du défaut et évitant ainsi le blocage de toutes les machines.
- Une administration noeud par noeud du réseau physique est possible à distance (par logiciel).
- On utilise un câblage de type « paires torsadées » (d'où la lettre T de 10 Base T), qui convient aussi actuellement à d'autres types de réseaux physiques.

Les réseaux Ethernet utilisent tous une **topologie logique en bus** (les machines sont vues par le réseau comme étant en parallèle) et 10 Base T n'échappe pas à la règle ; cependant, sa **topologie physique est l'étoile**, on dit alors parfois que sa topologie (globale) est le « bus étoilé ».

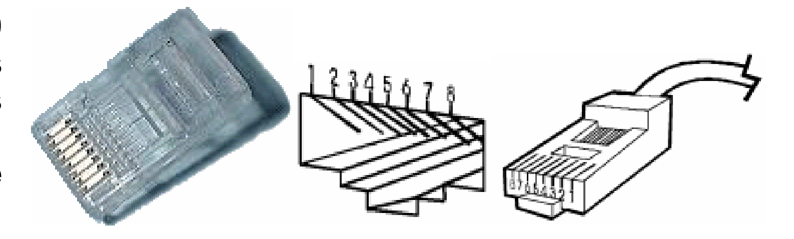


En réalité, les machines ne sont pas interconnectées directement, elles sont reliées individuellement aux entrées ou ports d'un concentrateur, appelé « Hub » (il a besoin d'alimentation secteur), qui simule intérieurement le bus. Dans les immeubles pré-câblés, il faut préalablement passer par une prise murale et par une armoire de brassage avant d'arriver aux Hubs.



On trouve diverses HUB 10 base T : simples, administrables par logiciel, capables ou non d'isoler un « port » défaillant,…

Les connecteurs utilisés en 10 base T ont la référence RJ45. Ils sont cousins de RJ12 utilisées aux USA en téléphonie.
Ils supportent « huit fils » (**quatre paires**)



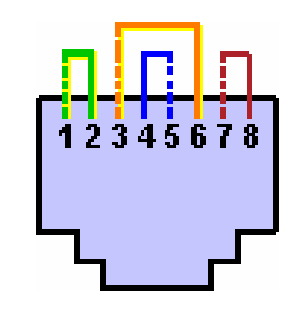
Le standard 10 Base T est normalement basé sur des câbles à deux paires torsadées non blindées dits « UTP » (Unshielded Twisted Pair).

Il existe aussi des câbles blindés (pour réseaux locaux) qui contiennent des paires torsadées ; ils peuvent être classés en deux catégories :

- Le blindage des câbles de la première catégorie les recouvre globalement et ne les protège donc que des interférences et des parasites extérieurs : les professionnels parlent alors d'écran plutôt que de blindage. C'est le cas des câbles blindés à paires torsadées qui sont équipés de connecteurs RJ45 ; on les appelle couramment « FTP » (Foiled Twisted Pair). Il n'est pas interdit d'installer de tels câbles en 10 Base T, notamment pour augmenter l'immunité aux perturbations ; leur efficacité contre les interférences et les parasites ambiants ne sera cependant effective que si les connecteurs RJ45 sont eux-mêmes blindés (une couche de métal les recouvre) et si les Hubs gèrent ce blindage (continuité de masse), ce qui n'est pas généralisé puisque hors du standard 10 Base T. Il est normal que les adaptateurs réseau, eux, ne gèrent pas le blindage s'il était connecté aux deux extrémités du câble (côté adaptateur et côté Hub), on pourrait constater un effet contraire à celui recherché appelé boucle de masse.
- L'écran global des câbles de la deuxième catégorie est complété par un blindage qui recouvre chaque paire individuellement ; il les protège de la diaphonie, c'est-à-dire de l'influence (involontaire) d'une paire vers les autres. Ces câbles, souvent appelés STE (Shielded Twisted Pair), sont plus encombrants et plus chers et ne sont pas utilisables en 10 Base T ; les câbles de descente utilisés en 10 Base 5 (AUI-AUI) entrent dans cette catégorie.

Le **10 Base T n'utilise que les paires 1&2 et 3&6**, mais il est conseillé d'installer des câbles à quatre paires afin de permettre une adaptation à tout type de standard, notamment le 100 Mb/s.

Chaque paire de fil possède une couleur : dans une paire, nous avons un fil de couleur torsadé avec son compagnon qui peut être, soit d'une couleur plus claire, soit blanc discontinu par la couleur.

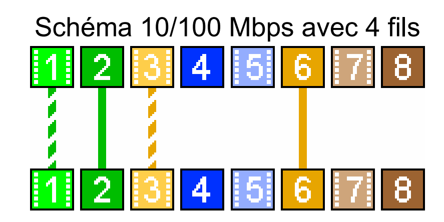


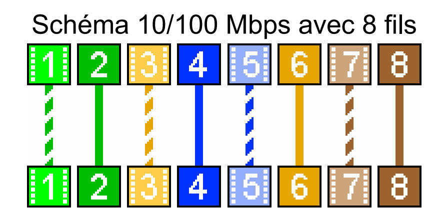
Ces paires sont souvent numérotées de la façon suivante :

N° de la Paire	Couleur principale	Broche	Couleur compagnon claire	Couleur compagnon discontinue
1	Bleu	4 & 5		
2	Orange	**3 & 6**		
3	Vert	**2 & 1**		
4	Brun (marron)	8 & 7		

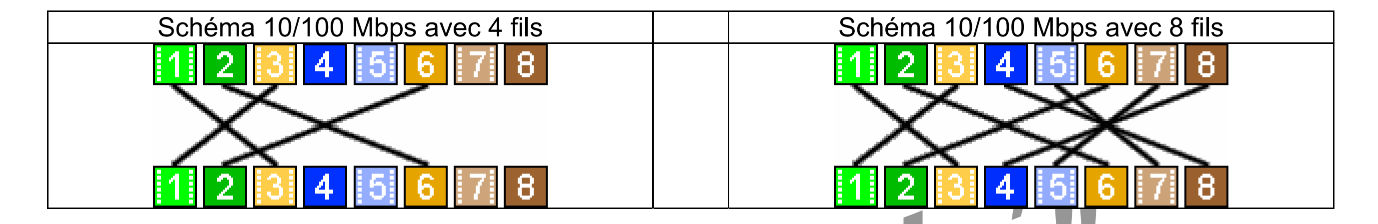
Broche	Hub (MDI-X)	Carte Réseau (MDI)
1	*RD+ (Réception)*	TD+ (Transmission)
2	*RD- (Réception)*	TD- (Transmission)
3	TD+ (Transmission)	*RD+ (Réception)*
4	Non utilisé en Éthernet. (Masse)	
5		
6	TD- (Transmission)	*RD- (Réception)*
7	Non utilisé en Éthernet. (Masse)	
8		

1.c.1 Brochage du câble droit - 4 ou 8 fils (10/100 Mbps) - Éthernet





1.c.2 Brochage du câble croisé - 4 ou 8 fils (10/100 Mbps) - Éthernet



Indépendamment du nombre de paires, de l'impédance (normalement 100 Ω), de la présence ou non d'un blindage, de la plus ou moins grande rigidité à la pliure, on classe les câbles à paires torsadées en catégorie, classe ou niveau (level), selon la bande passante.

La norme internationale ISO 11801 réglementant les installations de câblage, ainsi que les différentes normes nationales, définissent plusieurs catégories de composants. Les critères retenus sont l'atténuation et la para diaphonie, pour une largeur de bande donnée.

Ainsi la catégorie 5 certifie que les composants utilisés permettent un fonctionnement correct jusqu'à 100 MHz.

Critères de performances retenus pour les différentes catégories :

Catégorie	Certification	Utilisation
1	aucun critère de performances	Câble téléphonique ordinaire, utilisé pour le transport de la voix
2	certifié jusqu'à 1 MHz	Certifié pour le transport de données jusqu'à 4 Mb/s sur quatre paires torsadée
3	certifié jusqu'à 16 MHz	10 Mb/s - 10 Base T
4	certifié jusqu'à 20 MHz	16 Mb/s
5	**certifié jusqu'à 100 MHz**	**100 Mb/s**
6 / E	En cours de définition par l'ISO 11801, spécifie les composants et les performances du lien sur 100 mètres jusqu'à 200 MHz	

La **longueur maximale d'un segment** de câble situé entre une machine et un Hub est de **100 mètres**. La longueur minimale est de 2,5 m.

1.d 10 base F

Ethernet existe sur fibre optique, depuis 1992, sous trois variantes dont la plus courante est 10 Base FL.
Bien que la fibre permette d'atteindre des vitesses au moins dix fois supérieures, les équipements doivent se limiter à 10 Mb/s. Ceci est d'autant plus indispensable que 10 Base F est rarement utilisé de manière isolée et doit donc être parfaitement interopérable avec les autres réseaux Ethernet que l'on utilise dans l'entreprise.

La longueur totale d'un segment est de 2 Km.

2. Fast Ethernet 100 Mbits/s

Fast Ethernet ou 100 Base T (100 pour... 100 Mb/s) peut être considéré comme une extension d'Ethernet ; il utilise la même méthode d'accès (CSMA/CD), le même format de trame et la même topologie logique en bus (les trames sont envoyées, en parallèle, à l'ensemble des machines d'un même segment on dit que la bande passante est partagée entre les machines).
Cependant, on ne pourra évidemment pas faire du Fast Ethernet avec les éléments actifs (concentrateurs/Hub, adaptateurs réseau, etc.) conçus pour l'Ethernet classique à 10 Mb/s. On notera que les collisions sont toujours possibles (elles sont gérées exactement de la même façon) ; le débit réel, en situation, peut donc se révéler tout à fait inférieur aux 100 Mb/s théoriques comme il pouvait être inférieur aux 10 Mb/s avec l'Ethernet classique (on parle de 40 à 60 Mb/s), chutant notamment lorsque le nombre des utilisateurs qui parlent/trafiquent sur le réseau augmente.
Fast Ethernet est prévu exclusivement pour une topologie physique en étoile, à base de concentrateurs (Hub) 100 Mb/s spécifiques. On ne trouvera donc pas (saut sur des équipements mixtes 10/100 Mb/s) de câblage de type coaxial fin ou coaxial épais.

2.a 100 Base TX

100 Base TX est le sous-standard du Fast Ethernet le plus répandu car il représente l'évolution naturelle de 10 Base T.
Il utilise du câble à paires torsadées, non blindé (UTP), nécessairement de catégorie 5, équipé des classiques connecteurs RJ45.
Seules deux paires sont utilisées en 100 Base TX, les deux mêmes qu'en 10 Base T.

2.b 100 Base T4

100 Base T4 est moins courant. Il se satisfait au minimum de câbles non blindés de catégorie 3 munis des classiques connecteurs RJ45

Cependant, il exige d'utiliser ses quatre paires (torsadées) trois paires se partagent en parallèle la transmission du signal, ce qui demande moins de performances intrinsèques au câble, alors que la quatrième est dédiée à la détection des collisions. Il est donc censé reprendre tout câblage existant ; cependant, il peut y avoir deux difficultés les limites du 100 Mb/s concernant les distances maximales (comme pour 100 Base TX) et le fait que les paires complémentaires soient câblées effectivement et correctement sur les connecteurs et prises murales et qu'elles ne soient pas affectées à d'autres usages comme... la téléphonie.

2.c 100 Base FX

Cette variante de Fast Ethernet utilise la fibre optique (multimode).
En raison de son coût supérieur, 100 Base FX va surtout être mis en oeuvre comme autoroute, épine dorsale (backbone) pour fédérer (relier) les éléments actifs collectifs (concentrateurs, par exemple) d'un réseau 100 Mb/s ou mixte (10/100 Mb/s).
La fibre optique permet également d'allonger les distances sous Fast Ethernet, plutôt limité sur ce plan dans ses versions « cuivre ». Evidemment, la fibre (10 Base F, 100 Base FX, etc.) convient aussi tout particulièrement aux traversées de zones riches en perturbations et rayonnements électromagnétiques.

3. Interconnexion 10 Mbits/s et 100 Mbits/s

Rappelons que Fast Ethernet et Ethernet partagent méthode d'accès, format de trame et topologie logique. La plus simple des méthodes consiste à utiliser un concentrateur mixant les ports 10 Mb/s (10 Base T) et 100 Mb/s (100 Base TX) dont chaque port est bi-mode 10/100. Il est évident qu'on mettra, en priorité, les serveurs sur 100 Base TX.

4. Full Duplex

La plupart des réseaux classiques fonctionnent en **Half Duplex** les données circulent dans les deux sens (par exemple avec une paire pour l'émission et une paire pour la réception) mais **chacune à leur tour**, puisque les protocoles utilisés imposent un seul droit de parole simultané sur le réseau.

Les techniques de la commutation ont permis d'aller encore plus loin en développant des solutions **full duplex**, propriétaires puisqu'il n'y a aucune standardisation, qui permettent d'annoncer **20 Mb/s** (en fait 2 x 10 Mb/s) en Ethernet, 200 Mb/s (en fait 2 x 100 Mb/s) en 100 Base T. Elles font appel à des switching Hubs et à des adaptateurs réseau spécialement conçus pour accepter ce mode et sont surtout intéressantes pour les liaisons entre switchs et pour la connexion des serveurs très sollicités.

5. En résumé

Principaux réseaux physiques couramment utilisés :

Réseau physique	Vitesse	Distance
10 Base 2	10 Mbits/s	185 m par segment (30 nœuds max)
10 Base T	10 Mbits/s	100 m entre machine et Hub
100 Base TX	100 Mbits/s	100 m entre machine et Hub ainsi qu'inter Hubs
100 Base FX	100 Mbits/s	2 Km inter Hubs en mode Full Duplex

6. Liens internet

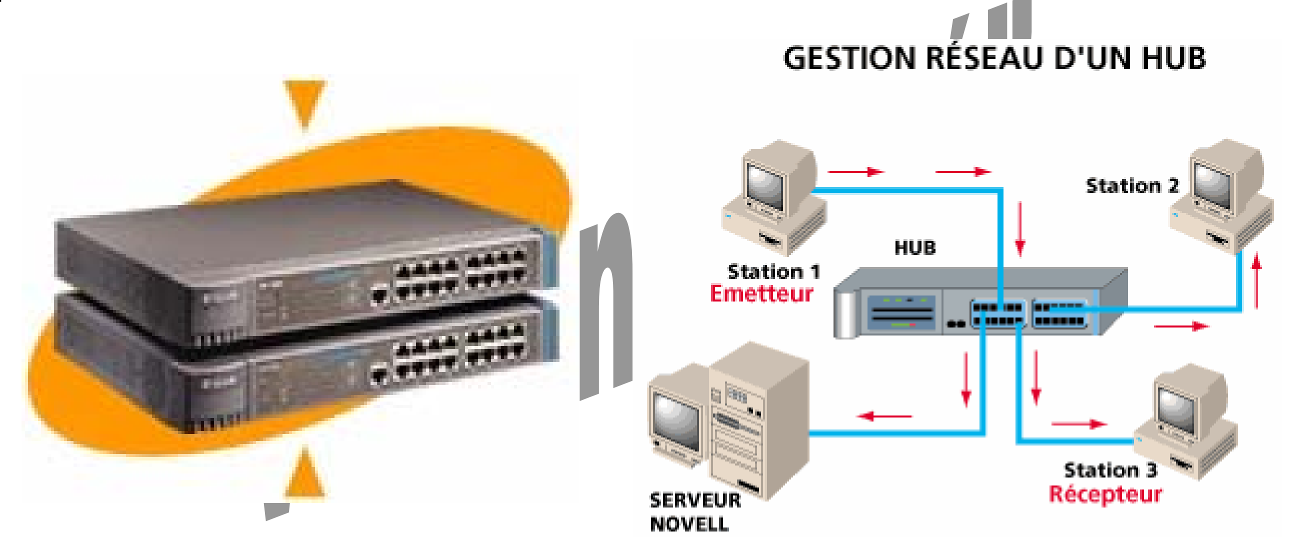
http://www.multimania.com/gowap/matos/partage/RJ45C.html

❑ Eléments actifs d'un réseau 10 base T, 100 base T : Hub, Switch

1. HUB

Les machines sont reliées individuellement aux entrées ou « port » d'un concentrateur appelé « HUB ».
Le HUB simule intérieurement le « bus ».

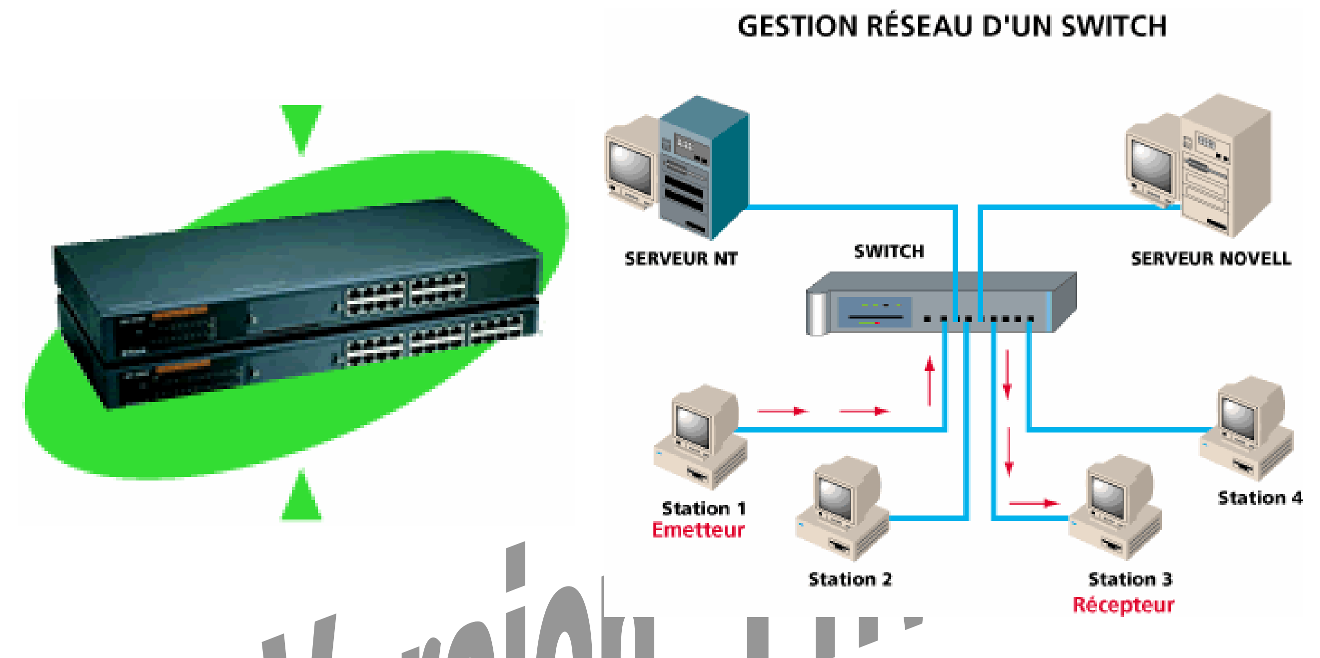
Les trames envoyées à destination d'une machine sont en fait reçues par toutes les machines même si elles sont seulement traitées par la machine à qui elles sont destinées (principe du BUS).
De plus la bande passante théorique de 10 Mbits/s ou de 100 Mb/s n'est disponible pour chaque machine mais partagée entre toutes les autres, puisqu'une seule machine à la fois peut normalement émettre et recevoir sur le réseau.



Si le Hub du réseau ne possède plus de port disponible, il est possible alors de connecter un nouveau Hub avec l'ancien (chaînage de Hub). En norme Ethernet, un maximum de 4 Hubs peut être installés de cette façon et en Fast Ethernet, c'est un maximum de 2. Pour contourner cette contrainte et augmenter la taille du réseau, il faut alors opter pour des Hubs empilables : vous pouvez alors empiler plusieurs Hubs pour augmenter le nombre total de ports, chaque pile de Hubs n'étant vue que comme un seul Hub.

2. SWITCH

Avec les concentrateurs-commutateurs, que l'on appelle le plus souvent Switched Hubs ou même tout simplement **Switchs**, les trames envoyées à une machine particulière sont directement aiguillées vers la machine destinatrice, en supprimant toute collision, la topologie logique n'est donc plus le bus mais l'étoile.



Le Switch scinde le réseau en autant de « sous-réseaux » qu'il a de ports et crée des liens privilégiés entre chaque élément connecté. Grâce à la fonction d'auto-apprentissage des adresses MAC, l'information envoyée à travers le Switch est directement dirigée vers la machine de destination.

De plus, chaque machine connectée à un port du Switch dispose d'une bande passante dédiée. Les machines connectées à un Switch peuvent travailler en full duplex c'est-à-dire qu'elles peuvent émettre et recevoir en même temps.

Décongestion du réseau :

Les données sont envoyées d'un port à un autre sans interférer sur les autres ports.

Augmentation de la bande passante :

Si le Switch fonctionne à 100Mbps, chaque port bénéficie d'une bande passante de 100Mbps.

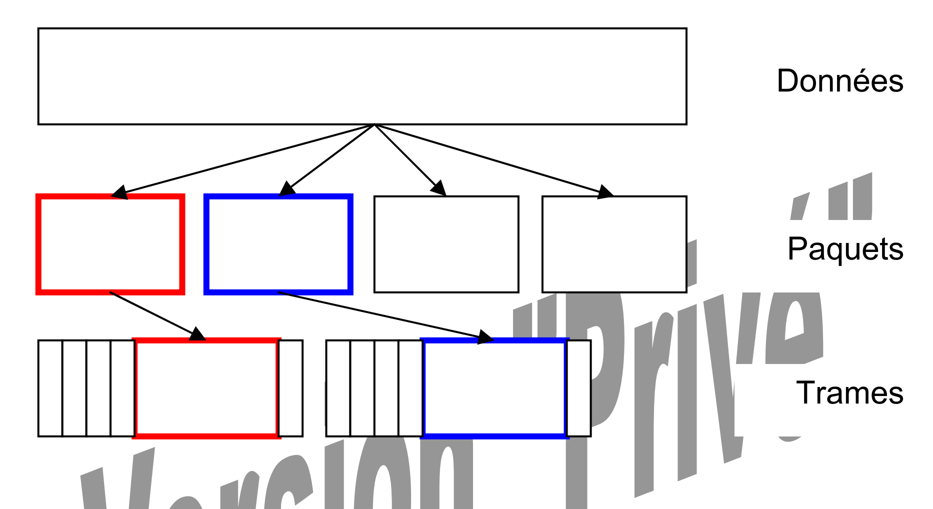
Accélération du transfert de données :

Le Switch permet des communications simultanées autant de fois que le nombre de ports du Switch divisé par 2. Chaque port est full duplex, ce qui permet d'émettre et de recevoir en même temps.

❑ Couche réseau Logique : les protocoles

<u>Protocole</u> : Description formelle de règles et de conventions régissant la manière dont les stations d'un réseau échangent des informations.

Le protocole est un élément déterminant. Il est couramment lié aux couches 3 et 4 du modèle OSI (transport et réseau). Il segmente les données en « paquets » qu'il place dans le champ « données » des trames créées par les couches physiques. Il établit les relations entre adresses logiques et physiques (MAC) de tous les destinataires, choisit l'itinéraire le plus approprié pour assurer leur acheminement (« routage ») et corrige les erreurs de transmission.



Les principaux protocoles LAN les plus utilisés en micro-informatique actuellement sont :

- NetBEUI
- IPX/SPX
- TCP/IP
- AppleTalk

1. NetBEUI

L'histoire de NetBEUI commence par NetBIOS (NETwork Basic Input Output System) ; ce dernier, qui fournit des services à divers niveaux OSI, a été conçu originellement par IBM comme interface de communication entre adaptateurs réseau et NOS.
NetBEUI (NetBIOS Extended User Interface) met en oeuvre ses services de niveau réseau-transport (couches n°3 et n°4) et descend aussi vers les couches basses. Les services de niveau Session de NetBIOS constituent un standard de fait comme points d'entrée des applications réseau et sont soit directement utilisés soit émulés.

NetBEUI est d'une mise en oeuvre simple (il se configure et se règle tout seul), il occupe peu de place en mémoire, son contrôle de débit et ses paramètres d'ajustage sont puissants, sa détection d'erreur est excellente.

Cependant, il présente quelques inconvénients. Il n'a aucune idée de ce qu'est une adresse logique ou réseau (notion de routage absente de la couche n°3) et fait se

reconnaître les noeuds du réseau en faisant appel à des services de couche 5 (Session) - il ne s'agit alors plus d'adresses réseau, mais de noms réseau -, ce qui ne facilite pas l'interconnexion inter réseau. Il a été conçu et optimisé pour les réseaux purement locaux (LAN) et il est mal adapté aux réseaux WAN.

Enfin, il est essentiellement supporté par IBM et Microsoft qui le proposent traditionnellement par défaut sur leurs NOS pour réseaux locaux

2. IPX/SPX

IPX/SPX a été proposé en 1983 par la société Novell pour NetWare, son système d'exploitation de réseau (NOS) ; il est dérivé du protocole XNS (Xerox Network System), conçu à la base pour les réseaux de minis de la société Xerox. IPX (Internetworking Packet eXchange) occupe la couche OSI n°3, tandis que SPX (Sequence Packet Interchange) occupe la couche n°4.

IPX/SPX est d'une mise en oeuvre assez simple (il se configure et se règle tout seul). Il sait ce qu'est une adresse logique ou réseau (il est dit « routable »), ce qui facilite l'interconnexion inter réseau. Il est plus performant en fonctionnement local LAN que TCP/IP et occupe très peu de place en mémoire, notamment sur les stations clientes utilisant MS-DOS.

Il est essentiellement utilisé par les produits Net Ware et compatibles qui ne proposent pas NetBEUI.

3. TCP/IP

TCP/IP (Transmission Control Protocol / Internet Protocol) est un ensemble de protocoles, développés au début des années 70 par le département américain de la défense afin de permettre l'interconnexion en réseau local de machines hétérogènes.
Etant antérieur au modèle OSI (comme les architectures SNA d'IBM, DSA de Bull, etc.), il n'est pas tout à fait conforme à ce dernier, notamment concernant le respect des couches et les en-têtes techniques des paquets. En simplifiant, on peut dire que IP occupe la couche n°3 et que TCP occupe la couche n°4 et déborde sur la couche n°5.
En fait, TCP/IP n'est pas qu'un protocole réseau-transport, c'est toute une architecture (souvent opposée à OSI) qui couvre des couches les plus basses aux couches les plus hautes, supporte et inclut des applications typiquement TCP/IP (messagerie Mail, transfert de fichier FTP, gestion de terminal virtuel Telnet, partage de fichiers NFS, administration distante des matériels SNMP, etc.) livrées ou non selon les implémentations.

Aujourd'hui, les couches TCP/IP appartiennent au noyau UNIX et sont donc standard sur les machines qui tournent sur cette famille de systèmes d'exploitation (OS). De plus en plus de plates-formes proposent désormais une implémentation TCP/IP, en standard (gratuite) ou en option (payante).

TCP/IP n'est pas un protocole propriétaire (il est indépendant de tout constructeur ou éditeur), ses spécifications sont publiques et ses sources logicielles sont quasi gratuites; il est devenu un véritable standard de fait vers lequel tous les constructeurs et éditeurs se

tournent. Il est reconnu comme le meilleur moyen actuel d'interconnecter des machines hétérogènes en LAN comme en WAN. On notera que c'est également le protocole du réseau mondial Internet, dont le nombre d'abonnés a suivi une progression spectaculaire ces dernières années.

TCP/IP n'a pas que des avantages. Sa configuration n'est pas automatique : le technicien est obligé de définir, manuellement et individuellement sur chaque machine, une adresse IP (donc logique/réseau et non physique/MAC) qui devra impérativement être unique sur tout le réseau (LAN ou WAN), ainsi que divers paramètres techniques complémentaires, ce qui est laborieux dès que le réseau a quelque importance. Les autres protocoles cités précédemment gèrent les adresses (ou noms pour NetBEUI) de manière dynamique, en attribuant celles-ci dès qu'un noeud se met à parler. On notera que la capacité de codage des adresses IP est actuellement limitée à 32 bits (forme: xxx.xxx.xxx.xxx), ce qui peut se révéler une limite insupportable pour les très grands réseaux comme Internet. Enfin, avec TCP/IP, le fait de passer d'Ethernet 10 Mb/s à 100 Mb/s ne multiplie pas par dix les performances (à cause de TCP).

Microsoft a intégré, dans son Windows NT Server, un service qui rend le paramétrage dynamique et complètement automatique ; il s'agit de Microsoft **DHCP** (Dynamic Host Configuration Protocol). Si un poste client (station cliente) est retiré du réseau (ce qui est souvent le cas avec les portables), son adresse IP est automatiquement libérée pour une nouvelle machine qui se connecterait ; le service DHCP attribuera au poste nomade une nouvelle adresse lors d'une reconnexion ultérieure. DHCP n'est pas la propriété de Microsoft, c'est une spécification issue de l'IETF (Internet Task Force) qui l'a définie pour faciliter l'administration de TCP/IP sur un WAN. Sans DHCP, il faut connaître l'adresse réseau d'un noeud pour s'y connecter. De plus, Microsoft propose WINS (Windows internet Name Services), qui permet sous TCP/IP d'attribuer des noms NetBIOS plutôt que des adresses logiques (en fait, il établit la correspondance entre les deux), ce qui est beaucoup moins abstrait.

4. AppleTalk

AppleTalk est un protocole réseau spécifique et intrinsèque aux machines Apple.

Conçu originellement pour fonctionner exclusivement sur le réseau physique LocalTalk d'Apple (réseau propriétaire intégré à toute machine Macintosh, comme AppleTalk, très simple à mettre en oeuvre mais limité à 230 Kb/s et à 32 noeuds physiques), il a été adapté sur les bases physiques Ethernet (avec pour nom EtherTalk).

En ajoutant le protocole AppleTalk à un serveur PC-intel fonctionnant sur une base physique Ethernet, on va lui permettre de parler le même protocole que les Macintosh ; cependant, pour que des partages de ressources et d'applications soient possibles et pour qu'on reconnaisse les noms de fichiers Macintosh, il faut que le NOS du serveur dispose de services spécifiques à l'environnement d'Apple (l'ajout d'AppleTalk seul ne suffit pas). On notera qu'il est aussi possible d'ajouter TCP/IP, récemment fourni en standard par Apple, aux machines Macintosh.

Fin du support